CORNELIUS P. McCARTHY (CM-3544)
CHEHEBAR DEVENEY & PHILLIPS
485 Madison Avenue Suite 1301
New York, New York 10022
Tel.: 212-532-8204
Cell: 914-629-0687
Fax: 212-753-8101
E-mail: cmccarthy@cdlawllp.com

PIERCE O'DONNELL (PO-5724)
GREENBERG GLUSKER FIELDS CLAMAN
& MACHTINGER
2049 Century Park East, 26th Floor
Los Angeles, California 90067
Tel.: 310-201-7558
Cell: 310-480-3366
Fax: 310-201-1792
E-mail: podonnell@greenbergglusker.com

Attorneys for Plaintiff
MICHAEL TERPIN

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

MICHAEL TERPIN, Plaintiff, -against- ELLIS PINSKY, as an individual; and DOES 1-20, Inclusive, Defendants.	Case No.: 20-CV-3557 (CS) (LMS) **FIRST AMENDED COMPLAINT FOR: (1) VIOLATIONS OF THE RACKETEER INFLUENCED AND CORRUPT ORGANIZATIONS ACT (RICO) (18 U.S.C. § 1962(C)); (2) CONVERSION; (3) MONEY HAD AND RECEIVED; (4) REPLEVIN; AND (5) PRELIMINARY AND PERMANENT INJUNCTION** **DEMAND FOR JURY TRIAL**

Plaintiff MICHAEL TERPIN, ("Plaintiff"), as and for his First Amended Complaint for claims for relief against defendants ELLIS PINSKY ("Pinsky") and DOES 1 through 20, inclusive ("Doe Defendants") (collectively, "Defendants"), based on personal knowledge as to his own acts and information and belief as to the acts of all others, alleges as follows:

INTRODUCTION

1. This case involves a sophisticated cybercrime spree against Plaintiff by an experienced criminal enterprise masterminded by a then 15-going-on-16-year-old high school student with the active participation of other individuals, including several other minors. The cybercrime enterprise, which for many years had hacked accounts of numerous individuals, stole and laundered tens of millions in cryptocurrency from Plaintiff. Working with confederates on multiple continents and on multiple heists, the ringleader of this scheme, Defendant Ellis Pinsky ("Pinsky"), has been a cyber-criminal since age 13 and has claimed to have stolen over $100 million in cryptocurrency from numerous victims over that time. At least one of his confederates has made similar multi-million dollar claims. Plaintiff Michael Terpin, a high-profile cryptocurrency pioneer, fell victim to Pinsky's criminal enterprise when, in early 2018, it stole nearly $24 million worth of cryptocurrency through a hack perpetrated by Pinsky and his gang of digital bandits (herein referred to as the "Enterprise").

2. Pinsky, who recently turned 18, has apparently graduated from a suburban New York high school and is set to attend college. In his early teens and along with confederates, he began hacking computers and phishing victims with the mission of accessing his victims' private accounts where they store cryptocurrency holdings, assets or private information. From those exploits he has reputedly obtained over $100 million. One of his and the Enterprise's major criminal activities has been engaging in SIM swaps—a type of hack described in greater detail below that involves accessing a victim's mobile telephone to gain access to personal information, such as two-factor authentication messages, to find information relating to cryptocurrency accounts.

3. One of Pinsky's partners was Nicholas "Nick" Truglia, a then 20-year-old New York hustler who, until recently, was imprisoned in Santa Clara County, California, is charged

with suspected grand larceny for stealing cryptocurrency, and is currently on bail awaiting criminal trials in the state court in California and in the federal court in New York. Federal authorities have indicted Truglia for stealing Plaintiff's cryptocurrency. Truglia's assignments from the Enterprise often included identifying victims, obtaining their cell phone and passcode numbers, conning the mobile phone carrier into giving him or another imposter a new SIM card, and then handing off the scam to Pinsky to execute the hack. Truglia is part of the Enterprise but not a Defendant in this action – Plaintiff has already sued Truglia in a separate action and obtained a judgment against him from the Los Angeles County Superior Court in the State of California.

4. Mr. Terpin's case is typical of the way in which the Enterprise operates in a coordinated manner to steal their victims' cryptocurrency. Pinsky, Truglia, and others in the Enterprise, who are sued herein as Doe Defendants, operated the Enterprise by dividing up their responsibilities. Some members of the Enterprise locate potential targets (preferably those, such as Mr. Terpin with large cryptocurrency holdings) and obtain information about their victims, such as telephone numbers and carriers. Members of the Enterprise then either impersonate the victims or coopt or bribe employees of the carriers to cooperate with the theft, forge identity papers for the victims, and then take over the victim's mobile telephone. Once in control of the telephone, Pinsky, Truglia, and other members of the Enterprise then roam openly through files of the victim and access and intercept two factor authentication messages until they located information about cryptocurrency holdings that allow them to take control of the cryptocurrency and exfiltrate such holdings into their own accounts.

5. It is believed that Pinsky met other members of the Enterprise in a chat room called the "Original Gangsters" or "OGUsers Forum." Based upon Plaintiff's investigations, including information from several informants (including a former accomplice of Pinsky's

referred to herein as "Individual X") and statements made by Pinsky and Truglia to informants, the Enterprise included numerous individuals both within and outside the United States. Plaintiff further alleges on information and belief that Pinsky was aided not only by Truglia, but by several other members of the Enterprise including "Accomplice A," "Accomplice B" and "Accomplice C" and other individuals.

6. Truglia has identified Pinsky and others as his confederates in cryptocurrency thefts, including that of Mr. Terpin. In several recorded conversations after the 2018 theft that were obtained by Plaintiff only in late December 2018, Truglia admitted how Plaintiff's cryptocurrency was purloined, described Pinsky's integral role in the theft, named other participants in the theft, and described how the proceeds of the theft were divided among the members of the Enterprise. Along with other highly incriminating evidence, Truglia's detailed account of Pinsky's penetration of Plaintiff's accounts and how he unlocked the unique secret to the passcodes for his crypto-wallets conclusively demonstrates that Pinsky was one of the hackers.

7. The financial crimes of Pinsky, Truglia, and their confederates in hacking others are no less insidious than bank robberies, credit card and bank fraud, and money laundering by drug traffickers and terrorists. They are all egregious crimes against society that evince an utter and callous disregard for the property and feelings of others. And they are deserving of the same severe punishment and public opprobrium.

8. If not before, the Enterprise began its criminal exploits when Pinsky was only 13 (several years before Plaintiff's SIM swap) and meets the requirements for a "criminal enterprise" under the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. § 1962(C). Although the full elements of Plaintiff's RICO claim are set forth below, they are briefly summarized here to provide context for the detailed allegations that follow.

9. First, the Enterprise engaged in numerous "predicate acts" and violations that constitute a pattern of racketeering under 18 U.S.C. § 1961(B) and (C) of RICO. These predicate acts include multiple and separate acts of (a) wire fraud under 18 U.S.C. § 1343 by the Enterprise each and every time it struck a new victim in transferring the money and cryptocurrency it stole through interstate commerce; (b) money laundering under 18 U.S.C. § 1956(a)(1)(B)(i) by the Enterprise laundering cryptocurrency through multiple transfers and use of "blenders" to try to render the stolen cryptocurrency untraceable; (c) aggravated identity theft under 18 U.S.C. § 1028(A)(a)(1) by the Enterprise impersonating the victims of their SIM swaps and bribing the employees of mobile carriers to transfer SIM cards and remove protections for such cards; and (d) extortion and grand larceny under New York Penal Law §§ 155.40 and 155.42 (as when Pinsky and other members of the Enterprise threatened Individual X and his family with physical violence if he did not cooperate with the Enterprise and pay substantial money to Pinsky).

10. Second, the Enterprise had an existence separate and apart from the hack it perpetrated on Mr. Terpin. As noted, the Enterprise began several years before it hacked Mr. Terpin and continued after Mr. Terpin was hacked. It included attempts by Pinsky and his accomplices, including Accomplice C, to destroy evidence and create a phony cover story by falsely blaming Truglia alone for all the hacks. As alleged herein, the Enterprise perpetrated criminal acts on numerous victims other than Mr. Terpin. As further evidence thereof, Pinsky's repeated boast that he obtained $100 million from his criminal activities represents a sum that he could not have reached had the Enterprise not had numerous other victims, even taking into account his share of the $24 million hack of Mr. Terpin and his share of a separate and distinct hack. Moreover, the efficient, precise and coordinated manner in which the Enterprise carried out the SIM swap of Mr. Terpin demonstrated an expertise in Pinsky and his accomplices that

could only have been obtained with practice and via numerous heists over an extended and lengthy period of time.

11. Third, the Enterprise was of a continuing nature. Given the inherently unlawful nature of the Enterprise, which engaged in repeated predicate acts of wire fraud, money laundering, aggravated identity theft and extortion, the risk of continuity of the Enterprise is deemed established under applicable Second Circuit law. *See United States v. Aulicino*, 44 F.3d 1102, 1111 (2d Cir. 1995); *GICC Capital Corp v. Tech. Fin. Group. Inc.*, 67 F.3d 463, 466 (2d Cir. 1995). Moreover, as alleged below, the illegal activity of the Enterprise is both an open-ended and closed-ended criminal enterprise.

12. The wholesome appearance of Pinsky and other members of the Enterprise is deceptive. Pinsky and his fellow Enterprise members are in fact evil computer geniuses with sociopathic traits who heartlessly ruin their innocent victims' lives and gleefully boast of their multi-million-dollar heists. As one of many examples, one victim lost all the money set aside for his daughter's college education. The apparent ringleader of the group, Pinsky, is constantly reaching out for the support of equally callous offenders who think nothing of stealing millions from their victims to live a life of conspicuous consumption. The Enterprise—in Mafia-like fashion—threatens others (such as Individual X) with physical harm to themselves and family members to coerce them to engage in illegal activities. Pinsky is reputed to have used his ill-gotten gains to purchase multi-million-dollar watches, illegal nightclub sprees at high end clubs in New York City (he is a minor), and private jet travel, while Truglia has himself rented private jets and played the part of a dashing playboy with young women pampering him.

13. Pinsky also has continually boasted to friends that he is invincible and would never get caught. In early 2019, Pinsky texted:

> "You think I'm fucking dumb. . . . I'm not fucking stupid. . . . I threw out

> all my shit [computers]. . . . Fuck that attorney [Terpin's lawyer]. They don't have shit on me. . . . You think I'm dumb enough to keep all my money in America. . . . [Truglia] is a dumb ass . . . and got caught."

14. Since the theft, Plaintiff has mounted an all-out, global effort to track down Pinsky, Truglia, and others to find evidence about their involvement in the theft of his cryptocurrency and in other criminal activities and hacks and to recover his assets. In a California lawsuit, Mr. Terpin obtained a writ of attachment for Truglia's assets, and later obtained a judgment against Truglia for almost $75.8 million. As Plaintiff increased the pressure, Pinsky began to panic. Following Terpin's lawyer calling Pinsky's mother on January 3, 2019, his mother contacting her lawyer, and Mr. Terpin's attorneys then presenting that lawyer with a draft complaint at a meeting on January 7, 2019, Pinsky himself made a series of devastating admissions in texts with an acquaintance who is an African-American. Among other things, he acknowledged that: "I'm well off I'm good I don't need extra money I'm set for life . . . You're a dumb nigger I could buy you and all your family . . . **I have 100 million dollars."** As evidence began to leak out about the Enterprise and Pinsky's role in it, Pinsky also cooked up a phony defense blaming Truglia alone for the hacks and had an accomplice attempt to get other members of the Enterprise to adopt that lie.

15. Since that date, Pinsky admitted his participation in the theft by making a payment to Plaintiff of cryptocurrency, cash, and a watch. On the one hand, the value of slightly over $2 million at the time of return represents a fraction of the amount for which Pinsky is responsible. On the other hand, however, it confirms Pinsky's involvement since there is obviously no other explanation for his possession of such funds or his delivery to Plaintiff of any amount.

16. Pinsky has redefined the conventional meaning of "spoiled brat." Pinsky is arrogant, remorseless, and accustomed to getting what he wants—private jet flights, luxury cars, and expensive accessories. Whether this evil mastermind's parents were recklessly negligent or worse in failing to monitor and control their wayward son remains to be seen.

17. The tables are now turned on Pinsky, Truglia, and their confederates in the Enterprise. Plaintiff will expose the secret dark side of their teenage counterculture of SIM swaps and cryptocurrency thefts that operate – with fellow hackers in the OGUsers' forum – beneath a seemingly wholesome facade. In view of Pinsky's boast that he has salted away $100 million in ill-gotten gains, nothing less than full restitution of Plaintiff's losses, plus interest, attorneys' fees, costs, and expenses, will satisfy Plaintiff that Defendants have adequately compensated him for his loss. And, an award of treble damages or punitive damages will send the appropriate message to Defendants and others that the epidemic of these types of SIM card attacks have real consequences and must immediately cease.

NATURE OF ACTION

18. This is an action for violation of the Racketeering Influenced and Corrupt Organizations Act ("RICO"), 18 U.S.C. §§ 1961-1968); conversion and conspiracy to commit conversion; money had and received; replevin; aiding and abetting unlawful conduct; and a preliminary and permanent injunction.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction of this civil action pursuant to 28 U.S.C. §§ 1332 (a) and 1367(a) and under the doctrine of pendent jurisdiction. This Court also has subject matter jurisdiction of this civil action pursuant to 28 U.S.C. Section 1332(a)(1) because this dispute involves citizens of different states and the amount in controversy exceeds $75,000, exclusive of interest and costs.

20. This Court also has personal jurisdiction over Defendant Pinsky. As alleged more fully below, each of the Defendants, acting in person or through their respective employees, agents and/or alter egos, has engaged in substantial, continuous, and systematic activities within the State of New York. Pinsky resides within the State of New York and this Judicial District. The claims sued upon arise out of Defendants' forum-related, unlawful activities directed towards Plaintiff.

21. Venue is proper in this Court under 28 U.S.C. §§ 1391(a)(2), (b)(2) and (c), because a substantial part of the events or omissions giving rise to Plaintiff's claims against Defendants occurred in this Judicial District and a substantial part of the property that is the subject of the action is situated within this Judicial District.

PARTIES

22. Plaintiff Michael Terpin is a citizen of the United States who has a residence in Los Angeles County, California. Mr. Terpin obtained wireless services from AT&T Mobility, Inc. ("AT&T") in Los Angeles County in the mid-1990s. Mr. Terpin is resident in California, Puerto Rico and Nevada. Mr. Terpin continued at all times relevant to the allegations herein to receive wireless services from AT&T for a telephone number with a Southern California area code.

23. Mr. Terpin is well known for his involvement with cryptocurrency. Cryptocurrency is digital or virtual currency designed as a medium of exchange in which encryption techniques generate units of currency that verify the transfer of funds through an encrypted and decentralized ledger called "blockchain." The blockchain records transactions and manages the issuance of new units of currency. Cryptocurrency is decentralized, operates independently of a central bank or other regulatory authority, and is often traded by parties through "exchanges." Once a transfer of cryptocurrency has occurred, it is impossible to trace or

reverse the transaction without possession of certain private and complex key numbers held only by the transferor.

24. Defendant Ellis Pinsky is an 18-year-old citizen of the United States residing with his mother in suburban New York. At the time in 2018 that he stole nearly $24 million of cryptocurrency holdings from Plaintiff, he was approaching his sixteenth birthday and was already highly adept in matters regarding computers, the digital world, phishing, cryptocurrency holdings, cryptocurrency theft, the blockchain, and laundering cryptocurrency holdings and money.

25. Non-party Nicholas Truglia is a former resident of New York, New York, who until recently was incarcerated in the Santa Clara County jail in California on charges of grand theft, identity theft, unauthorized computer access, and other felony charges. Truglia is currently out on bail for charges in the California state court system and a federal indictment in the Southern District of New York involving the theft of Plaintiff's $24 million cryptocurrency.

26. Plaintiff is ignorant of the true names and capacities of defendants sued herein as DOES 1-20, inclusive, and therefore sues these defendants by such fictitious names. As alleged below, individuals whom Plaintiff has preliminarily identified as Accomplice A, Accomplice B, and Accomplice C have taken various roles in the Enterprise. When the true names of these and other individuals is ascertained, Plaintiff will amend this Complaint to allege their true names and capacities.

27. Plaintiff is informed and believes and, on that basis, alleges that Defendants, and each of them, were and are the agents, employees, representatives, principals, partners, co-conspirators, joint venturers and/or alter egos of each of the other Defendants, and/or otherwise were acting in concert with each of the other Defendants, and in such capacity or capacities participated in the acts or conduct alleged herein. They were also acting within the scope of such

relationship, such that each should be held liable for the acts of the other. In addition, they are each in some manner responsible for the damages suffered by Plaintiff and the relief sought here as alleged below.

COMMON ALLEGATIONS

28. This lawsuit is about the unauthorized and wrongful taking from Plaintiff of nearly $24 million in cryptocurrency by Pinsky and other members of the Enterprise. Pinsky and his fellow gang members, including Truglia, and Accomplices A, B and C, were at the center of the plot to gain unlawful access to Plaintiff's accounts and information via bribery and/or impersonation and identity theft, and to steal and to launder his cryptocurrency, all using communications in interstate commerce.

SIM SWAPS AKA SIM-JACKING

29. The theft here was made possible by the increasingly prevalent practice of unauthorized SIM swaps. This is an illegal maneuver by which a hacker takes over a victim's cellular phone account to intercept messages to facilitate the theft of funds (often cryptocurrency) and transfer such funds to the hacker or the hacker's accomplices or to cryptocurrency accounts under the hackers' control. Increasingly publicized, SIM swaps have become a focus of federal and state law enforcement authorities.

30. A "SIM" or "Subscriber Identity Module" (also known as a "SIM card") is a small card inserted into a mobile device enabling the device to communicate with the service provider. A SIM contains data necessary to make a successful connection between the mobile phone and the telecommunication provider. SIM cards store files that are used to uniquely identify them.

31. A "SIM swap" is a practice whereby a hacker gains access to a victim's telephone account or number in order to intercept communications, including text messages, to the mobile

telephone. The process is also referred to as "SIM-jacking." A perpetrator of a SIM-jack typically arranges through bribery of someone (often a carrier employee) with access to customer information at the carrier to change the SIM card assigned to a user to a telephone under the control of the hacker or the hacker's accomplices. Once the SIM transfer has occurred, the hacker uses the hacker's phone to impersonate the victim with service providers, such as e-mail providers, and uses the victim's phone number to request changes to account settings and to reset passwords to take control of the victim's accounts.

32. Perpetrators of SIM swap fraud, such as Pinsky, Truglia, Accomplices A, B and C and other participants in the Enterprise, intercept "2-Factor Authentication" (or "2FA") messages sent to the victim's telephone. 2FA is frequently used as a security mechanism for authentication purposes. Perpetrators of SIM swaps, including members of the Enterprise, intercept the messages to gain access to the accounts owned by the victim, including cryptocurrency accounts or other accounts providing access to such accounts. Once the perpetrator gains access to the account, the perpetrator transfers the funds in such accounts to an account or accounts controlled by the perpetrator or confederates.

33. The perpetrators of SIM swap fraud – SIM-jackers – specifically target victims owning cryptocurrency because of the nature of cryptocurrency transactions and seek to steal the identity of such victims. The digital assets embodied by cryptocurrency (such as Bitcoin or Ethereum) are a medium of exchange using cryptography to secure the transaction. Typically, the holder of cryptocurrency has both a "public" and a "private" key or address that the holder uses to receive, transfer, or use cryptocurrency. The private key, which is individual to the owner of the cryptocurrency, is used to write in the public ledger to transfer cryptocurrency. Because the key can be used to "spend" cryptocurrency, owners typically keep such keys secure.

Such keys are complex. For example, in the case of Bitcoin, a 256-bit private key may contain 64 characters consisting of numbers and capitalized and uncapitalized letters.

34. Once a transfer of cryptocurrency has occurred, it cannot be reversed. Although the transaction is displayed in a public ledger, it is not readily possible to identify the transferor or transferee without knowing the parties' private keys. Cryptocurrency thus makes an attractive target for perpetrators of SIM swap fraud, such as the Enterprise, because the perpetrators can transfer stolen digital assets to accounts that are not readily traced or reversed and can be accessed anywhere in the world free from government regulation or inspection.

THE JANUARY 7, 2018 SIM-JACK

35. Plaintiff makes the allegations of Paragraphs 36-56 on information and belief.

36. Pinsky and Truglia, with the active assistance of Accomplices A, B and C and other members of the Enterprise, orchestrated and efficiently carried out the SIM swap of Plaintiff's cell phone on January 7, 2018 by bribing an AT&T employee or contractor to obtain a SIM card connected to Mr. Terpin and then intercepting messages directed to Mr. Terpin so that they could steal his cryptocurrency, which they did on January 7-8, 2018.

37. Some time ago, a group of young video game players—with participants in the United States and Great Britain—formed a user group called "Original Gangsters" or "OGUsers." In time, this moniker proved apt as they morphed into the nucleus of a sophisticated criminal enterprise operating in North America, Europe, and Asia. Their racket was theft of cryptocurrency by means of SIM swaps. Each of the dozen or more gangsters in the Enterprise had assigned roles, including identifying the victims, obtaining their cell phone and passcode numbers, impersonating and stealing the identity of the victims, conning or bribing mobile phone carriers' employees into giving the imposter a new SIM card, and handing off the personal identity information to the other members of the Enterprise who executed the hack and laundered

the cryptocurrency holdings into Bitcoins or fiat money in accounts under their own control that could be transferred to anonymous wallets.

38. The Enterprise's hack of Mr. Terpin fits this pattern. As summarized in the examples in the following chart, the members of the Enterprise divided up the responsibilities for their January 7, 2018 cryptocurrency hack of Michael Terpin and the subsequent laundering of the cryptocurrency, almost all of which involved electronic communications:

Date	**Events and Participants**
On or before January 7, 2018	Pinsky and Accomplice A identify Michael Terpin as the target of a SIM swap hack. Information is exchanged among them about Plaintiff and the plan via electronic communications.
On or before January 7, 2018	Pinsky secures via electronic communication(s) the agreement of Jamil Smith, an employee or contractor of AT&T, to obtain the SIM card for Mr. Terpin's mobile phone in exchange for several hundred dollars.
On or before January 7, 2018	Jamil Smith transfers via electronic communication to a member of the Enterprise, believed to be Accomplice B, the necessary information for the Enterprise to use the SIM card for Mr. Terpin's mobile phone and removes protection on the SIM card, including PIN.
On or before January 7, 2018	Either before, concurrently, or shortly after delivery of the SIM card, Pinsky pays the bribe amount to Jamil Smith via electronic communication
January 7, 2018	Accomplice B installs Mr. Terpin's unprotected SIM card in a phone controlled by him, which cuts off Terpin's access to his phone.
January 7, 2018	Pinsky and possibly other members of the Enterprise, including Accomplice A, begin via electronic Internet connections to attempt to access Terpin's accounts. As and when necessary to bypass passwords, Pinsky and possibly other members of the Enterprise via electronic communications request password resets and/or are asked for 2FA information.
January 7, 2018	Accomplice B, who is in control of a phone that is acting as Mr. Terpin's phone by virtue of the SIM-swap, intercepts password reset and 2FA messages that are intended for and sent to Mr. Terpin via electronic communications.
January 7, 2018	Each time Accomplice B intercepts such a message intended for Mr. Terpin, Accomplice B promptly forwards the messages via electronic communications to Pinsky.
January 7, 2018	Using the 2FA and password reset messages forwarded by Accomplice B, Pinsky and possibly other members of the Enterprise access accounts of Mr. Terpin via electronic Internet communications until they reach Mr. Terpin's cryptocurrency holdings.
January 7-8, 2018	Pinsky and other members of the Enterprise including Accomplice A steal nearly $24 million of Mr. Terpin's cryptocurrency holdings (Triggers, Steem and Skycoin) by

Date	Events and Participants
	giving instructions via electronic communications to transfer such holdings from Mr. Terpin's accounts to accounts and/or wallets held and controlled by the Enterprise.
January 7-8, 2018	Pinsky and other members of the Enterprise transfer via electronic communications the Triggers from Mr. Terpin's accounts worth almost $22 million to five cryptocurrency accounts under their control at the cryptocurrency exchange Binance.
January 7-8, 2018	Pinsky and other members of the Enterprise via electronic communications instruct Binance to convert the Triggers in their accounts to Bitcoin (BTC).
January 7-11, 2018	Pinsky, Truglia, Individual X and Accomplice B and others in the Enterprise via electronic communications instruct Binance to move the BTC out of their five separate accounts to private cryptocurrency wallets controlled by the members of the Enterprise. Although Binance has refused to provide information to Mr. Terpin about its investigation of these matters, it is believed that these transfers include the transfers of over 30 BTC on January 7, 2018, over 80 BTC on January 8, 2018, over 90 BTC in a separate transfer on January 8, 2018, and over 5 BTC on January 9, 2018, and that there were other similar transfers on these and subsequent days until virtually all of the proceeds had been moved out of Binance.
January 10, 2018	Individual X, at Pinsky's instruction, attempted via electronic communication to transfer 50 BTC from Binance to a private wallet but misdirected the transfer.
After January 7, 2018	The members of the Enterprise, via electronic communications, successfully launder the Steem cryptocurrency.
After January 7, 2018	The members of the Enterprise are unsuccessful in laundering the Skycoin cryptocurrency.
After January 11, 2018	Pinsky and other members of the Enterprise via repeated and numerous electronic communications move and further launder the cryptocurrency in their private accounts in hundreds of additional transfers.
After January 11, 2018	Pinsky and the other members of the Enterprise divide the proceeds of the hack of Mr. Terpin with Pinsky, Accomplice A and Truglia receiving greater amounts and other members of the Enterprise receiving smaller amounts.
After January 11, 2018	Pinsky, Truglia and other members of the Enterprise, via electronic communications, convert BTC in their private accounts to cash and use the cash and/or BTC to purchase luxury goods, services and entertainment.

39. On or prior to January 7, 2018, Accomplice A, who with Pinsky appears to be a ringleader of the Enterprise, identified Mr. Terpin as the target of the hack.

40. On or about January 7, 2018, Pinsky himself called, texted or otherwise electronically communicated with an employee or contractor of AT&T named Jamil Smith (with whom he was previously acquainted), and secured Smith's agreement to obtain the SIM card for

Mr. Terpin's phone in exchange for a bribe of several hundred dollars. In a separate electronic communication that occurred prior to, concurrent with, or shortly after delivery of the SIM card, Pinsky sent the bribe payment to Smith.

41. On or about January 7, 2018, Jamil Smith transferred the SIM card to Accomplice B (most likely through the Internet) with the information needed to activate Mr. Terpin's SIM card in a phone controlled by Accomplice B. Smith's actions at that time included removing the PIN that protected the SIM card from being used by anyone other than Mr. Terpin.

42. On January 7, 2018, Accomplice B installed the SIM card in a phone controlled by him. On January 7, 2018, Plaintiff's phone went dead. The SIM-jackers for all intents and purposes had hijacked Plaintiff's digital identity.

43. On or about January 7, 2018, Accomplice B, who had been involved in previous SIM swaps, controlled the phone with Mr. Terpin's SIM card and intercepted electronic 2FA messages on the phone meant for Mr. Terpin and forwarded them to Pinsky and Accomplice A.

44. Through their interception of 2FA messages, on or about January 7, 2018, Pinsky and the other members of the Enterprise were successful in finding information about Mr. Terpin's accounts and cryptocurrency holdings sufficient to control the accounts and the cryptocurrency in them.

45. On January 7 and 8, 2019, Pinsky and his accomplices engaged in multiple electronic transactions across state lines and internationally by which they accessed and stole nearly $24 million worth of cryptocurrency from Mr. Terpin in the form of Triggers, Skycoin, and Steem.

46. On and after January 7, 2018, the members of the Enterprise transferred Mr. Terpin's stolen cryptocurrency electronically to five cryptocurrency accounts under their control at the cryptocurrency exchange firm Binance.

LAUNDERING PLAINTIFF'S STOLEN COINS

47. Like drug cartel money, stolen cryptocurrency holdings are dirty or "hot" because they may raise suspicion as to their origins (particularly if they are possessed by a teenager like Pinsky). Cryptocurrency thus may be very difficult to spend if it is not either washed or converted to other forms of readily-spendable currency. The Enterprise thus had to move and launder the three types of coins they stole from Plaintiff, *i.e.*, 3,000,000 Triggers, 12,500 Steem, and 20,000 Skycoin.

48. On and after January 7, 2018, Pinsky and other members of the Enterprise instructed Binance to convert the Triggers that they had transferred to the separate accounts under their control at Binance to Bitcoin (BTC), which is one of the best-known and readily usable forms of cryptocurrency

49. On January 7-11, 2018, Pinsky, Truglia, Individual X, Accomplice B and other members of the Enterprise instructed Binance to move the Bitcoin out of the five separate Binance accounts they had established to private cryptocurrency wallets controlled by them. (A cryptocurrency wallet is a physical medium or program storing the public and private keys needed to trade cryptocurrency.) Each transfer by Pinsky and the other members of the Enterprise entailed multiple electronic communications across state lines or internationally using computers or other devices and the Internet.

50. The members of the Enterprise, via electronic communications, gave numerous instructions to Binance that resulted in almost all of the proceeds of the Triggers stolen from Mr. Terpin being moved from Binance to private wallets. As examples, there were electronic communications directing the transfer of over 30 BTC on January 7, 2018, of over 80 BTC on January 8, 2018: of over an additional 90 BTC on January 8, 2018: and of over 5 BTC on January 9, 2018. In addition, Individual X (at Pinsky's instruction) attempted on January 10,

2018 via electronic communications to transfer 50 BTC in two separate transactions from Binance, but misdirected the transfers.

51. Plaintiff alleges that the members of the Enterprise made additional transfers of Bitcoin from Binance to private wallets. Plaintiff does not yet have access to the specific details of these additional transfers, which are in the possession of the Enterprise, the members of which processed these transactions and transfers in their own accounts after stealing Mr. Terpin's cryptocurrency. Such information is also believed to be in the possession of Binance, but Binance has refused to provide Plaintiff with information about these transactions. Given the value of the Triggers at the time they were taken from Mr. Terpin (which was $22.7 million, the equivalent of about 1,350 Bitcoin), there were additional transfers from Binance to the members of the Enterprise.

52. After Pinsky and the other members of the Enterprise had transferred the Bitcoin in their Binance accounts to private wallets, they continued to move and further launder the cryptocurrency in literally hundreds of additional transfers in January 2018 and for several months thereafter. All of these multiple transfers were done electronically.

53. At about the same time and continuing throughout 2018, Pinsky, Truglia and other members of the Enterprise converted Bitcoin to cash to purchase luxury goods, services and entertainment. Indeed, Truglia conspicuously flaunted his wealth, according to Chris David, as did Pinsky.

54. Defendants attempted to launder, and in fact laundered, the Steem coins as well.

55. Laundering the Skycoin proved more difficult. Defendants opened an account at the C2CX exchange in the name of a Florida State student, which was apparently a stolen identity. As further alleged below, on or after January 7, 2018, Pinsky enlisted the assistance of Individual X to establish an account at C2CX for the purpose of laundering the cryptocurrency.

Plaintiff further alleges on information and belief that the Enterprise proceeded to convert the Skycoin into Bitcoin at substantially below market valuations, but it was ultimately unable to move the proceeds off the exchange.

56. Sometime in early 2018, the members of the Enterprise divided the proceeds of the hack of Mr. Terpin amongst themselves with Pinsky, Accomplice A and Truglia receiving greater amounts of the stolen cryptocurrency and others receiving smaller amounts. Pinsky, as one of the ringleaders of the Enterprise's hack of Mr. Terpin, played a significant role in determining how the proceeds were split.

PINSKY AND TRUGLIA ADMIT THEIR CRIMES

57. The evidence of Pinsky's, Truglia's and the Enterprise's culpability for organizing and directing scores of SIM swaps and thefts, collectively totaling well over $100 million of cryptocurrency holdings, including Plaintiff's nearly $24 million, is overwhelming and irrefutable.

58. The involvement of Pinsky and the Enterprise in the theft of Mr. Terpin's cryptocurrency was confirmed by revelations regarding the involvement of Truglia in the hack and by subsequent investigations. In November 2018, Truglia was arrested for the theft of $1 million of cryptocurrency holdings owned by someone other than Plaintiff. On December 18, 2018, the Santa Clara County Superior Court held a bail hearing for Truglia. In this hearing, the Court cited evidence that on January 7, 2018, which the Court states was the same date that Terpin lost more than $20,000,000 through a SIM swap, Truglia told someone named Ryan O'Keefe that he had stolen a cryptocurrency wallet with 20 million in it. On the same date, Truglia texted a friend: "I'm a millionaire. I'm not kidding. I have 100 Bitcoin."

59. On January 7, 2018, the average price of one Bitcoin varied between $16,033 and $17,244. *See* *https://www.livebitcoinnews.com/bitcoin-price-analysis-january-7th-2018-bears-*

control/. On the date of the Terpin SIM swap, Truglia boasted that "today my life changed forever," and he offered to hire "porn star escorts" and take his friends to the Super Bowl.

60. Truglia has been identified in a California criminal case as the perpetrator of numerous SIM swap frauds. In a December 2018 hearing in Truglia's case, the prosecution cited an investigatory report revealing that Truglia had used telephone accounts obtained through SIM swaps to register new cryptocurrency accounts, including accounts on Coinbase, Gemini, and Binance. Truglia also engaged in money laundering efforts after his SIM swaps by moving his stolen cryptocurrency through multiple addresses, breaking up the stolen amounts into multiple segments of smaller amounts, structuring his transactions to avoid reporting requirements, and otherwise taking steps to avoid due diligence and suspicion. As Mr. Terpin learned in late December 2018, Truglia has boasted about his cybercrimes to many friends.

61. Likewise, Pinsky has been identified as Truglia's partner in multiple SIM swap frauds, which was how Mr. Terpin first learned of Pinsky. In 2018, after the Terpin hack but prior to his arrest, Truglia implicated Pinsky in several conversations recorded by a friend. Critically, however, Mr. Terpin did not learn that Truglia had done so, and therefore did not know of Pinsky's involvement, until late December 2018. In a declaration that month under penalty of perjury, Chris David quoted the following admissions by Truglia from a September 2018 conversation between the two of them:

(a) How Pinsky and he hacked Terpin to steal his $24 million worth of Cryptocurrency holdings;

(b) How Pinsky and he laundered cryptocurrency holdings out of the blockchain into cash;

(c) Truglia has an account at the Gemini exchange and took out $1,200,000;

(d) Truglia committed tax fraud;

(e) Truglia saw records indicating that in December 2017, Pinsky had $70 million; and

(f) One of their victims, Plaintiff, is too "dumb" to be able to figure out what happened and trace the laundered cryptocurrency holdings.

62. In another conversation on September 9, 2018 (which Mr. Terpin also did not learn of until late December 2018), Truglia related the following to a mutual friend:

(a) He will never be caught hacking/stealing because he is so good at it—literally, "how are they going to prove . . . my story [his defense] wrong?";

(b) "Nobody can get me in trouble. Nobody can put me in jail. I would bet my life on it, actually"; and

(c) As of September 2018, Truglia had $60 million of Bitcoin.

63. In still another 2018 conversation (which Mr. Terpin learned of in late December 2018), Truglia admitted that:

(a) He told the police that he had $60 million when they came to his apartment;

(b) He had stolen all his money and had not legitimately accumulated his wealth;

(c) He was a computer hacker and stole his victims' cryptocurrency holdings and that this was thrilling for him—"the thrill of the game"—which he would never stop doing—even if there were no money involved; it was all "a mind game";

(d) His partner was named Ellis Pinsky, and Pinsky had stolen between $70 and $80 million through hacking of multiple victims and was a professional thief;

(e) He, Truglia, is a "Robin Hood" who robs from the rich but does not give to the poor;

(f) Pinsky and Truglia do hacking and SIM swapping by Truglia locating the victims through social engineering and Pinsky intercepting 2FA messages to find out information about accounts;

(g) Truglia's "biggest" SIM swap was Plaintiff Michael Terpin for $24 million, and Pinsky was his partner; and

(h) Pinsky took proceeds from the $24 million.

64. In mid-August of 2018, before he went to jail, Truglia further admitted his guilt for purloining Plaintiff's $24 million of coins. Remarkably, on his public Twitter account (@erupts) at Twitter.com, Truglia admitted six times that he "Stole 24 million," referring to Plaintiff's cryptocurrency holdings. As with other similar communications, Mr. Terpin did not learn of this communication until late December 2018.

65. On information and belief, Plaintiff alleges that Pinsky himself also has admitted that he is a cybercriminal. He has told friends that, since he was 13, he has stolen over $100 million worth of cryptocurrency through scores of hacks, and boasted of hundreds of thousands in cash stored in his bedroom in his mother's home. Indeed, when Pinsky repaid in 2019 a portion of the sum that had been stolen from Plaintiff, it included a cash payment consistent with Pinsky's boast.

66. Pinsky fancies himself as some kind of Super Boy who is beyond the reach of the law and impervious to Plaintiff's efforts to hold him liable for the $24 million heist. This brash egoist has texted:

> "You think I'm fucking dumb . . . I'm not fucking stupid . . . I threw out all my shit [computers] . . . Fuck that attorney [Terpin's lawyer]. They

> don't have shit on me. . .You think I'm dumb enough to keep all my money in America . . . [Truglia] is a dumb ass . . . and got caught."

67. In the same text session where he is declaring himself invincible, Pinsky demonstrated the wisdom of the adage that "pride comes before a fall." A wannabe Master of the Universe, Pinsky wrote to an African-American: "I'm well off I'm good I don't need extra money I'm set for life . . . You're a dumb nigger I could buy you and all your family . . . **I have 100 million dollars."**

68. More recently, after being confronted by Plaintiff about his involvement, Pinsky (with the advice of sophisticated legal counsel) sent cryptocurrency, cash, and a watch to Plaintiff without any conditions. As Pinsky and Plaintiff have no other connection to one another other than as stated herein, there was no reason to repatriate these items—worth roughly $2 million at the time—other than to make a partial repayment of what he had stolen from Terpin. Pinsky has thereby further admitted his complicity.

PINSKY'S EXTORTION OF INDIVIDUAL X

69. Plaintiff makes the allegations in Paragraphs 69-74 regarding Pinsky's extortion of Individual X on information and belief.

70. On or about January 3, 2018, Pinsky first threatened Individual X, whom he had recruited to be part of the Enterprise. On or about January 3, 2018, Individual X participated in a group twitter chat with Pinsky and other members of the Enterprise and certain third persons. On that same date, after the chat ended, Pinsky sent a private message to Individual X that he, Pinsky, was angry that Individual X had included individuals in the chat who should not have been on the call. Pinsky at that time then threatened Individual X that if he did not want his mother dead he should pay Pinsky one thousand dollars' worth of any cryptocurrency Thereafter, Accomplice C, a participant in the chat, confirmed Pinsky's threat to Individual X.

After further threats in or about the same time, in which Pinsky claimed that he had spoken with Individual X's mother at her office and after Pinsky had rejected several offers of payment, Pinsky agreed to have Individual X pay Pinsky in Zclassic (which is a type of cryptocurrency), which Individual X then did, and Pinsky offered to help with Individual X's portfolio.

71. On or about January 7, 2018, Accomplice C and Pinsky separately contacted Individual X and asked him to establish a verified Binance account in return for Pinsky supposedly aiding him to recover the money he had sent to Pinsky. Plaintiff further alleges that, because of the timing of the request, this was one of the Binance accounts the Enterprise established for the transfer of Mr. Terpin's stolen cryptocurrency. Individual X then opened the Binance account and deposited Triggers in the account on both January 7 and January 8, 2018 and (as further instructed by Pinsky) requested Binance to convert the Triggers to Bitcoin over a number of days. On or about January 8, 2018 Pinsky and others in the Enterprise then instructed Individual X to transfer the Bitcoin in Individual X's Binance account to personal wallet accounts under their control. At or about the same time, Pinsky and members of his Enterprise further asked Individual X to establish an account on C2CX for laundering Mr. Terpin's Skycoin.

72. On January 9, 2018, Pinsky told Individual X that he would have to transfer his Binance account balance to a dark web Bitcoin site name Bitblender. Pinsky further told Individual X that he was destroying his--Pinsky's--computer. On January 10, 2018, Pinsky told Individual X that he would have to transfer funds on his own without Pinsky's help. Individual X on January 10, 2018 mistakenly transferred 50 Bitcoin to an account other than Pinsky's. When Pinsky learned of this, he told Individual X that he would not receive any money from the transfers and instructed him to destroy all files relating to the transfer and to never message Pinsky on the same account again.

73. Apparently enraged by Individual X's mistake, Pinsky then repeatedly threatened Individual X and attempted to extort the misdirected cryptocurrency from him. For example, in or about February 2018, Pinsky told Individual X to sell drugs to repay Pinsky's lost money. Pinsky also threatened Individual X by stating "Do u understand that if u did this to like a mafia or something you'd be dead by now [,] right?" In all, Pinsky demanded that Individual X pay Pinsky back hundreds of thousands of dollars at the rate of $3,000 to $4,000 a week.

74. On or about January 9, 2019 (after Truglia's arrest and almost immediately after Mr. Terpin's lawyer had presented Pinsky's lawyer with a copy of a draft complaint on January 7, 2019), Accomplice C texted Individual X stating that "It's about to be over" and that "someone snitched on" Pinsky. Accomplice C further stated that Pinsky had "framed it on someone else" and that everyone was to get "the story straight" or "we can get fucked." When asked what the "story" was, Accomplice C told Individual X that "basically there's this guy named Nick, he paid us to let him use our Binance accounts" and that Nick "added his own 2FA onto the accounts." Accomplice C stated that he was providing this story "just in [] case any[t]hin[g] were to happen." On information and belief, the references to "Nick" refer to Truglia and any suggestion that Accomplice C and Individual X may not have known Truglia despite each of them having roles in the hack of Mr. Terpin is consistent with a classic hub-and-spoke criminal enterprise model in which persons such as Pinsky and other ringleaders are at the hub of wheel and control numerous spokes of other co-conspirators.

OTHER ACTIONS OF THE PINKSY CRIMINAL ENTERPRISE

75. Plaintiff makes the allegations in Paragraphs 76-77 on information and belief.

76. Pinsky and Accomplice A, who were apparent leaders of the Enterprise, were involved in SIM swaps and hacks other than that of Mr. Terpin. Plaintiff further alleges that Pinsky had used Accomplice B on numerous occasions and had committed other hacks with

Accomplice A. Truglia, who undoubtedly was involved in hacks other than that of Mr. Terpin, repeatedly stated in his statements to Chris David in 2018 before he was arrested (and that were first known to Plaintiff only in December 2018) that Pinsky had frequently used social engineering ploys to go after disgruntled employees of mobile carriers to assist in SIM hacks. Moreover, the coordinated nature of the attack on Mr. Terpin indicates that the Enterprise was experienced in SIM swap hacks. Truglia further expressed skepticism in these conversations that Pinsky, whom he believed had $70-80 million from his hacks, had or would "retire" because hacking was a "game" for him (as indeed it was for Truglia himself). Truglia also called Pinsky in these conversations a "professional thief" even though Pinsky at the time was only 16 years old, and further stated that Pinsky had stolen tens of millions of dollars and had more money than Truglia himself. He also stated that Pinsky engaged in hacks "all of the time."

77. In 2017, and prior to the hack of Terpin, Pinsky was involved in another hack, the specific identity of which has previously been provided to counsel for Pinsky. That separate hack involved the theft of more than was taken from Mr. Terpin. Less than one month after that separate hack, Pinsky had cryptocurrency directly traceable to the hack in wallets known to be owned and controlled by Pinsky, and it is believed that Pinsky also owned and controlled the wallets where the proceeds of this hack were initially transferred. Separately, Pinsky made statements claiming to take responsibility for this major hack. In addition, for Pinsky to net the total of $100 million he has repeatedly claimed to hold, another hack of significant quantity would likely to have occurred, even given the number of Pinsky's SIM swaps and hacks of other victims.

/ / /

/ / /

/ / /

MR. TERPIN'S INVESTIGATIONS AND EXTRAJUDICIAL COMMUNICATIONS WITH PINSKY

78. Plaintiff did not begin to learn of Pinsky's involvement in this SIM-jacking until late December 2018. On January 3, 2019, soon after Mr. Terpin learned about Pinsky's involvement, Mr. Terpin's lawyers contacted Mr. Pinsky's mother and were then directed to John Siffert, Esq., who represented Mr. Pinsky.

79. On January 7, 2019, counsel for Mr. Terpin provided information regarding Mr. Terpin's claims against Pinsky to Mr. Siffert, including a draft complaint against Pinsky alleging RICO and the pendent state claims alleged herein. Discussions ensued between counsel in the following months. Pinsky's counsel urged Plaintiff not to file any lawsuit and gave assurances that Pinsky was cooperating with Plaintiff. During this same time period, Pinsky delivered cryptocurrency, cash, and a watch to Mr. Terpin, with a value at the time of about $2 million. After the return of this money, Pinsky's counsel continued to indicate that Pinsky was cooperating and that he desired to enter into a settlement agreement that would include the entry of a substantial judgment against Pinsky. And, for an extended period of time, the parties' counsel engaged in discussions about such an agreement. During these discussions, Pinsky's counsel repeatedly stressed the importance of delaying any judgment until the Fall of 2020 so that, should it become public, it would not interfere with Pinsky's college applications. While Pinsky's counsel expressed Pinsky's claimed concern about how he would manage to pay such a large judgment, it was never suggested at any time that Pinsky denied that he was involved the theft of Mr. Terpin's cryptocurrency; to the contrary, numerous statements were made that Pinsky could only have known by virtue of being involved as alleged herein. Based on the assurances from Pinsky's counsel that the parties were engaging in good faith settlement communications as reflected by the acknowledgments of Pinsky's involvement and cooperation

and based on the repeated pleas and requests that Plaintiff defer filing and work with Pinsky to find a resolution, Plaintiff delayed filing and engaged in extended discussions with Pinsky's counsel.

80. On April 24, 2020, Pinsky's lawyers communicated that Pinsky would not sign the agreement that had been drafted and that it contained multiple "deal-breakers." Understanding for the first time since the discussions had begun that there would not be a settlement, and now suspicious as to whether Pinsky ever intended to settle and that the drawn out negotiations had merely been a ruse to stall and delay the filing of the complaint, Plaintiff proceeded to promptly move forward with initiating litigation and filed the complaint in this action on May 7, 2020.

TERPIN'S DAMAGES

81. Terpin's cryptocurrency holdings that are the subject of this proceeding are valued in the sum of at least $23,808,125 consistent with applicable damages law.

82. Plaintiff is entitled at a minimum to interest on the losses, if not greater losses as a result of his inability to use his cryptocurrency holdings to invest the proceeds.

83. In seeking to recover his money, Plaintiff will have incurred substantial attorney's fees, costs, and expenses in a sum to be proven at trial, and in any event no less than $1,000,000.

84. Plaintiff is entitled to recover from Defendants at least $23,808,125 (before trebling or punitive damages), subject to credits given consistent with applicable law for any amounts recovered by Plaintiff, plus interest and attorneys' fees consistent with applicable law.

NECESSITY OF INJUNCTIVE RELIEF

85. As noted above, Pinsky has admitted that he has $100 million of stolen money, presumably in a mix of cash and cryptocurrency. He also reportedly had substantial cash stashed

in his bedroom, which was reconfirmed by his inclusion of at least some portion of that cash with the partial sum that he repaid in 2019.

86. Defendants have proven to be skillful professionals at using the internet for stealing and laundering coins and money. They are as dangerous with a computer as armed bank robbers are with guns.

87. Due to the nature of cryptocurrency and Defendants' mastery of cybercrime, Pinsky's assets, including the amounts taken from Plaintiff, could readily be dissipated and lost absent injunctive and other relief preventing any transfer.

FIRST CLAIM FOR RELIEF

(Against All Defendants for Violations of Section 1962(c) of the Racketeer Influenced and Corrupt Organizations Act (RICO), 18 U.S.C. § 1962(c))

88. Plaintiff realleges and incorporates by reference the allegations of Paragraphs 1 through 87 above as if fully set forth herein.

89. This claim for relief arises under 18 U.S.C. § 1962(c) and is asserted against Defendants Pinsky and DOES 1-20.

90. Pinsky, non-party Truglia and each of the Doe Defendants, for purposes of this particular cause of action, is or has been a "person" employed by or associated with an enterprise engaged in, or the activities of which affect, foreign or interstate commerce (the "Enterprise"), and as such, has conducted or participated, directly or indirectly, in the conduct of such Enterprise's affairs through a pattern of racketeering activity as described below.

91. For the purpose of this particular cause of action under Section 1962(c), Plaintiff alleges on information and belief that the Enterprise consists of Defendant Pinsky, non-Defendant Truglia, Accomplices A, B and C, the Doe Defendants and others whose names are not yet known to Plaintiff. The members of the criminal enterprise, whose chief members

included Pinsky and Accomplice A, engaged in and coordinated numerous criminal activities, including SIM swaps and other hacks. Pinsky himself was engaged in hacks since he was 13, which was several years before he and his cohorts are alleged to have hacked Mr. Terpin. Moreover, as alleged herein on information and belief, the Enterprise perpetrated numerous SIM swaps and hacks other than the SIM swap of Mr. Terpin's cryptocurrency. Indeed, Pinsky boasted that he had made $100 million, which means that either he engaged in a major hack, such as the one alleged in Paragraphs 75-77, or in numerous smaller hacks, which is consistent with Truglia's statement to Chris David after Mr. Terpin's hack that Pinsky did hacks "all of the time" and had not retired.

92. Plaintiff alleges on information and belief that since at least 2015 Defendants Pinsky, non-defendant Truglia, Accomplices A, B and C and Defendants DOES 1-20 and other Enterprise members, knowingly, intentionally, and unlawfully, aided and abetted, and conspired with each other, to devise, or intend, multiple coordinated schemes to defraud cryptocurrency holders and investors and others (including Plaintiff), by which they illegally stole their victims' identities in order to illegally obtain and acquire control of victims' cryptocurrency and other accounts, and to launder the proceeds of these accounts and to transfer such proceeds to accounts under their control. All of these actions were undertaken through multiple electronic communications and through interstate commerce and internationally. These actions constitute multiple violations of federal statutory law, including wire fraud (18 U.S.C. § 1343), money laundering (18 U.S.C. § 1956(a)(1)(B)(i)) and acts of aggravated theft under 18 U.S.C. § 1028(A)(a)(1) and are thus predicate acts constituting racketeering activity under 18 U.S.C. § 1961(B)

93. In furtherance of its scheme to defraud, and in order to achieve its objectives, the Enterprise knowingly, intentionally, and unlawfully aided and abetted to commit, attempted to

commit, conspired to commit, did commit, and caused to be committed, the herein enumerated overt and/or predicate acts of racketeering activity to illegally steal money from multiple victims, including Plaintiff, through SIM swaps, hacks and other subterfuges and to subsequently launder and retain such money.

94. On information and belief, for several years prior to Mr. Terpin's hack and continuing to the present, for the purpose of executing the Enterprise's scheme to defraud, Defendant Pinsky, non-Defendant Truglia, and Accomplices A, B and C and other members of the Enterprise unlawfully obtained information about multiple victims' mobile phone accounts, including information about security codes and other personal information, and bribed personnel at mobile carriers to obtain such information. The Enterprise then used such information, in combination with false identifications and information obtained through phishing or the Dark Web, to impersonate and steal the identity of multiple victims and through multiple electronic communications in interstate commerce to port over a victim's telephone number to a phone under the control of the Enterprise. The Enterprise used victims' phones to intercept messages to the victim, including 2FA messages, and accessed the victim's files and accounts to obtain information about cryptocurrency holdings, including private keys. Through this scheme, the Enterprise gained control of multiple victims' accounts, including cryptocurrency wallets or other accounts, and exfiltrated victims' cryptocurrency to accounts under their own control. The Enterprise further laundered the proceeds of their thefts to attempt to hide their identity. All of the actions of the Enterprise involved multiple communications through Interstate commerce through electronic means. The scheme perpetrated on Terpin by Defendants Pinsky, non-defendant Truglia, Accomplices A, B and C, and Defendants DOES 1-20, as alleged in this complaint, is typical of the Enterprise's *modus operandi*, but is only one example of the multiple criminal acts engaged in by the Enterprise.

95. The scheme perpetrated by the Pinsky and other members of the Enterprise, including non-defendant Truglia, Accomplices A, B and C, and DOES 1-20 took place in interstate commerce within the United States. Through the conduct described above, in furtherance of the scheme to defraud Terpin and other victims, the members of the Enterprise knowingly, intentionally, and unlawfully, aided and abetted and conspired with each other to violate, and did violate 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1956(a)(1)(B)(ii) (money laundering) and 18 U.S.C. § 1028(A)(a)(1) (aggravated identity theft).

96. Upon information and belief, Plaintiff further alleges that Pinsky and other members of the Enterprise threatened and extorted members of Enterprise and others, including Individual X, by threatening to kill or harm Individual X and a member of Individual X's family in order to extort money from Individual X. For example, Pinsky threatened to harm Individual X's mother and Individual X himself if he did not pay Pinsky cryptocurrency or did not return the misdirected cryptocurrency or sell drugs to raise money to pay him back. Pinsky also threatened Individual X by referencing what the Mafia would do to him in a similar situation. Such actions constitute extortion under New York Penal Law § 155.40 (grand larceny and extortion in second degree) and § 155.42 (grand larceny in first degree)). These violations of New York state law constitute additional predicate acts under 18 U.S.C. § 1961(A) because they constitute extortion and are subject to imprisonment under state law for more than one year.

97. Through the conduct described above, Defendants Pinsky, non-defendant Truglia, Accomplices A, B and C and Defendants DOES 1-20 and other Enterprise members, knowingly, intentionally and unlawfully, aided and abetted, conspired to, and each of them in fact did, conduct or participate, directly or indirectly, in the conduct of the Enterprise's affairs, through a pattern of multiple unlawful actions in violation of 18 U.S.C. § 1343 (wire fraud); 18 U.S.C. § 1956(a)(1)(B)(ii) (money laundering); 18 U.S.C. § 1028(A)(a)(1) (aggravated identity theft);

New York Penal Code § 155.05(2)(E) (extortion); and New York Penal Code § 155.40 (grand larceny and extortion in second degree); and § 155.42 (grand larceny in first degree. As a proximate cause of the Defendants' violations, Plaintiff was injured in his property inasmuch as he has been the object of theft of his property in violation of law.

98. The injuries suffered by Plaintiff Michael Terpin are reasonably estimated to be in the amount of at least $23,808,125, with interest accruing from the date each component of said sum was converted by Defendant, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff.

99. Pursuant to 18 U.S.C. § 1964(c), Plaintiff shall recover threefold the damages sustained in an amount of at least $71,415,375 (*i.e.*, $23,808,125 x 3), with interest accruing consistent with applicable law, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff. In 2019, a Los Angeles County Superior Court Judge assessed such treble damages against Truglia for his participation in the theft of Plaintiff's cryptocurrency and entered a $75.8 million judgment against him.

100. Pursuant to 18 U.S.C. § 1964(c), Plaintiff Michael Terpin is entitled to reasonable attorneys' fees, expenses, and costs in a sum to be proven at trial, and in any event no less than $1,000,000.

SECOND CLAIM FOR RELIEF

(Against All Defendants for Conversion and Conspiracy to Commit Conversion)

101. Plaintiff realleges and incorporates by reference the allegations contained in Paragraphs 1 through 100 above as if fully set forth herein.

102. At all times mentioned above, Plaintiff was, and still is, the owner and was, and still is, entitled to the possession of cryptocurrency valued in the sum of at least $23,808,125 consistent with applicable damages law.

103. On or about January 7, 2018, Defendants Pinsky, non-defendant Truglia, accomplices A, B and C and Defendants DOES 1-20 took and conspired to take the property described above from Plaintiff's possession in the manner described above and converted the same to their own use.

104. As a proximate result of the wrongful conduct of Defendants Pinsky, non-defendant Truglia, Accomplices A-C and Defendants DOES 1-20 as alleged above, Terpin has been damaged in the sum to be proven at trial, but at least $23,808,125, with interest accruing from the date each component of said sum was converted by Defendant, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff.

105. As a further proximate result of the acts alleged above, Terpin has also expended substantial sums of time and money in pursuit of the sums converted by Defendants. Terpin is presently incurring such amounts in an attempt to recover his converted property. The full amount and extent of those damages are presently unknown. Plaintiff will seek leave to amend this complaint when the full extent and amount of said damages have been ascertained.

106. Defendants Pinsky and DOES 1-20 have engaged in despicable conduct as alleged above with an intent to injure Terpin and to subject him to cruel and unjust hardship in conscious disregard of his rights, and these actions were done fraudulently, maliciously and oppressively. Terpin is therefore entitled to punitive or exemplary damages against Defendants in an amount sufficient to punish and make a public example of each of the Defendants.

THIRD CLAIM FOR RELIEF

(Against All Defendants for Money Had and Received)

107. Plaintiff realleges and incorporates by reference the allegations of Paragraphs 1 through 106 above as if fully set forth herein.

108. Defendant Pinsky and DOES 1-20 received money belonging to Terpin in the amount of a sum to be proven at trial, but at least $23,808,125 at that time. Defendants Pinsky and DOES 1-20 benefitted from the receipt of that money. Under principles of equity and good conscience, Defendants should under no circumstances whatsoever be permitted to keep that money.

109. The whole of this sum has not been paid back to Plaintiff, and there is now due, owing, and unpaid – as money had and received – the sum to be proven at trial, which is at least $23,808,125, with interest accruing from the date each component of said sum was converted by Defendants, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff.

FOURTH CLAIM FOR RELIEF

(Against All Defendants for Replevin)

110. Plaintiff realleges and incorporates by reference the allegations of Paragraphs 1 through 109, above, as if fully set forth herein.

111. Plaintiff is, and at all times material herein was, the owner of personal property described as the cryptocurrency holdings identified above.

112. Plaintiff is, and at all times material herein was, entitled to immediate and exclusive possession of his cryptocurrency holdings.

113. During and as a direct and proximate result of Defendants' wrongful possession and retention of his cryptocurrency holdings, Plaintiff has suffered the loss of the use and enjoyment of them as well as additional damages in an amount to be proven at trial but no less than $23,808,125, with interest accruing from the date each component of said sum was converted by Defendants, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff.

114. Neither Pinsky nor any other Defendant has returned to Mr. Terpin all that the Enterprise has stolen from Plaintiff.

115. Plaintiff is entitled to immediate return and possession of his cryptocurrency holdings.

116. In doing the acts alleged above, Defendants acted with oppression, fraud, and malice and with the intent to defraud Plaintiff. Accordingly, Plaintiff is entitled to an award of punitive and exemplary damages against Defendants in a sum to be proven at time of trial.

FIFTH CLAIM FOR RELIEF

(Against All Defendants for a Preliminary and Permanent Injunction)

117. Plaintiff realleges and incorporates by reference the allegations of Paragraphs 1 through 116 as if fully set forth herein.

118. Defendants' possession and control of Plaintiff's cryptocurrency holdings and money, and the substantial threat of loss through transfers to unknown accounts or persons, is causing and will continue to cause Plaintiff great and irreparable harm, for which Plaintiff has no adequate remedy at law.

119. Plaintiff is therefore entitled to a preliminary and permanent order enjoining and restraining Defendants Pinsky and DOES 1-20, and their agents, servants, employees, confederates, co-conspirators, aiders and abettors, and representatives from engaging in, committing, or performing, directly or indirectly, any and all of the following acts: accessing, expending, disbursing, transferring, assigning, pledging, encumbering, concealing, laundering, washing, or in any manner whatsoever disposing of the whole or any part of the cryptocurrency holdings and cash belonging to Plaintiff.

/ / /

/ / /

DEMAND FOR JUDGMENT

WHEREFORE, Plaintiff prays for judgment against Defendants, and each of them, as follows:

1. For the value of the property converted in the sum to be proven at trial, but at least $23,808,125, subject to credits given consistent with applicable law for any amounts recovered by Plaintiff;

2. For interest thereon at the legal rate from the date of the conversion of each component of the foregoing sum;

3. For additional damages for time and money properly expended in pursuit of the converted property, according to proof;

4. For an order requiring Defendants Pinsky and DOES 1-20, jointly and severally, to return to Plaintiff all assets, funds, and other property derived from such transactions, as well as any benefits or profits derived therefrom, and to pay Plaintiff any consequential damages caused by these transactions;

5. For an order compelling Defendants Pinsky and DOES 1-20 to reconvey legal title of Plaintiff's cryptocurrency holdings to Plaintiff;

6. For an order requiring Defendants Pinsky and DOES 1-20, and their agents, servants, employees, confederates, co-conspirators, aiders and abettors, and representatives to be enjoined during the pendency of this action, and then permanently enjoined after conclusion of this action, from engaging in, committing, or performing, directly or indirectly, any and all of the following acts: accessing, expending, disbursing, transferring, assigning, pledging, encumbering, concealing, or in any manner whatsoever disposing of the whole or any part of the cryptocurrency holdings and cash belonging to Plaintiff;

7. For punitive or exemplary damages in an amount sufficient to punish Defendants Pinsky and DOES 1-20 and make a public example of them;

8. For treble damages pursuant to 18 U.S.C § 1964(c);

9. For attorney's fees pursuant to 18 U.S.C. § 1964(c);

10. For costs of suit incurred herein; and

11. For such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiff demands trial by jury on all claims for relief for which a jury trial is appropriate.

DATED: September 11, 2020

CHEHEBAR DEVENEY & PHILLIPS

and

GREENBERG GLUSKER FIELDS CLAMAN & MACHTINGER LLP

By: /*s*/
CORNELIUS P. McCARTHY

By: /*s*/
PIERCE O'DONNELL

Attorneys for Plaintiff
MICHAEL TERPIN